



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/719,460

12/11/2000

Tomoyuki Asano

09812.0656

8319

22852

7590

05/31/2006

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER  
LLP

901 NEW YORK AVENUE, NW  
WASHINGTON, DC 20001-4413

EXAMINER

TRAN, TONGOC

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

C

**Office Action Summary**

Application No.

09/719,460

Applicant(s)

ASANO ET AL.

Examiner

Tongoc Tran

Art Unit

2134

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --****Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09 March 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1, 4, 6-28, 31, 33-55, 58, 60-82 and 87-107 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 4, 6, 28, 31, 33-55, 58, 60-82 and 87-107 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. This office action is in response to Applicant's amendment filed on March 9, 2006. Claims 1, 6-10, 15-19, 28, 34-37, 42-46, 55, 58, 60-82, 85 and 87-107 have been amended. Claims 1, 4, 6-18, 31, 33-55, 58, 60-82 and 87-107 are pending.

### ***Response to Arguments***

2. In light of Applicant's amendment, claims 1, 28, 55 and 82 rejected under 35 U.S.C. 112 second paragraph have been withdrawn.

Applicant's arguments with respect to amended claims (remark, pages 62-63) have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 4, 6-28, 31, 33-55, 58, 60-82, 85 and 87-107 are rejected under 35 U.S.C. 103(a) as being unpatentable over Traw et al. (U.S. Patent No. 6,542,610) in view of Jones (U.S. Patent No. 5,412,730).

In respect to claim 1, Traw discloses an information processing system comprising:

A first information processing apparatus and a second information processing apparatus, the first information first information processing apparatus comprising:

An interface having an isochronous transmission mode in which a transmission band is ensured and a transmission control means for controlling encrypted data in the transmission band and then transmitted in the isochronous transmission mode via the interface (e.g. col. 4, lines 39-58, col. 6, lines 34-40 and col. 9, line 53-col. 10, line 5).

Wherein the transmission control means executes, prior to data transmission, a protocol for performing mutual authentication and sharing a plurality of encryption keys with the second information processing apparatus, to which the encrypted data is to be transmitted, and from which an authentication request is to be received, and

Wherein the first information processing apparatus encrypts the data following said authentication request from the second information processing apparatus (see col. 4, lines 40-65); and

the second information processing apparatus comprising:

An interface having the isochronous transmission mode in which a transmission band is ensured and a receiving control means for controlling reception of encrypted data received by the second information processing apparatus from the first information processing apparatus (see col. 9, lines 53-66 and col. 11, lines 25-36),

Wherein the encrypted data which is received in the isochronous transmission mode via the interface is decrypted using the encryption key, wherein the receiving control means executes, prior to data reception, a protocol for performing mutual authentication and sharing a plurality of encryption keys with the first information

Art Unit: 2134

processing apparatus, from which the encrypted data is to be received, and to which an authentication request is to be transmitted, and wherein the second information processing apparatus decodes the data following an authentication request to the first information processing apparatus (see col. 4, lines 39-65 and col. 11, lines 25-36).

Traw does not explicitly disclose the encryption key used for decrypting the content is generated by a second random number generated by the second information apparatus. However, Jones discloses a pseudo-random number generator are employed at both the transmitting and the receiving stations to supply a encryption keys to both the encryptor and the decryptor (see Jones col. 1, lines 36-53). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement generation of encryption key used for decryptor in a second processing apparatus for decrypting the content data for the advantage of without these key being transmitted over the transmission facility (see Jones, col. 1, lines 41-42).

In respect to claim 4, Traw and Jones disclose the information processing system as claimed in claim 1, wherein the first information processing apparatus and the second information processing apparatus are connected with each other via an interface conforming to the IEEE (the Institute of Electrical and Electronics Engineers) 1394 standard, for transmitting data requiring the assurance of a transmission band in an isochronous transmission mode and for transmitting related data relating to the data in an asynchronous transmission mode (e.g. Traw, col. 10, lines 27-34).

In respect to claim 6, Traw and Jones disclose the information processing system as claimed in claim 1 wherein the second information processing apparatus generates two random numbers and transmits them to the first information processing apparatus, the first information processing apparatus generates two random numbers and transmits them to the second information processing apparatus, the first information processing apparatus generates an encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key used for encrypting the data to be transmitted in the second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number, and the second information processing apparatus generates an encryption key used for decrypting the data transmitted in the isochronous transmission mode and an encryption key used for decrypting the data transmitted in the second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number (e.g. Traw, col. 6, lines 1-66).

In respect to claim 7, Traw and Jones disclose the information processing system as claimed in claim 6, wherein the first information processing apparatus transmits data P generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, to the second information processing apparatus, the second information processing apparatus transmits data Q generated on the basis of the information indicating the validity of the

apparatus itself, the generated random number and the received random number, to the first information processing apparatus, the first information processing apparatus generates an encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data Q, and the second information processing apparatus generates an encryption key used for decrypting the data transmitted in the first transmission mode and an encryption key used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data P (e.g. Traw, col. 6, lines 1-67).

In respect to claim 8, Traw and Jones disclose the information processing system as claimed in claim 7, wherein the second information processing apparatus generates two random numbers R1 and R2 and transmits them to the first information processing apparatus, the first information processing apparatus generates two random numbers S1 and S2 and transmits them to the second information processing apparatus, the first information processing apparatus transmits data P generated on the basis of information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing

apparatus, the second information processing apparatus transmits data Q generated on the basis of information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the first information processing apparatus, the first information processing apparatus generates an encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and the second information processing apparatus generates an encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode and an encryption key K'2 used for decoding the data transmitted in the second transmission mode in the case where data P' generated on the basis of the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P (e.g. Traw, col. 6, lines 1-67).

In respect to claim 9, Traw and Jones disclose the information processing system as claimed in claim 8, wherein the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the first transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1, and generates the encryption key K2 used for



encrypting the data to be transmitted in the Second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, and the second information processing apparatus generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 used for decrypting the data transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 (e.g. Traw, col. 6, lines 1-67 and col. 7, lines 5-55).

In respect to claim 10, Traw and Jones disclose the information processing system as claimed in claim 9, wherein the first information processing apparatus transmits data P generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus, the second information processing apparatus transmits data Q generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the second information

Art Unit: 2134

processing apparatus, the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and the second information processing apparatus generates the encryption key K' used for decrypting the data transmitted in the isochronous transmission mode and the encryption key K'2 used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P (e.g. Traw, col. 6, lines 1-67, col. 7, lines 5-55).

In respect to claim 11, Traw and Jones disclose the information processing system as claimed in claim 9, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using a bit value of a part of the result of calculation of the unidirectional function (e.g. Traw, col. 6, lines 1-67, col. 7, lines 5-55).

In respect to claim 12, Traw and Jones disclose the information processing system as claimed in claim 11, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q and the data P', using a bit value of a part of the result of calculation of the unidirectional function (e.g., Traw, col. 6, lines 1-67, col. 7, lines 5-55).

In respect to claim 13, Traw and Jones disclose the information processing system as claimed in claim 11, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using a feast significant n bits of the result of calculation of the unidirectional function (e.g. Traw, col. 6, lines 1-67 and col. 7, lines 5-55).

In respect to claim 14, Traw and Jones disclose the information processing system as claimed in claim 13, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q' and the data P', using a most significant m bits of the result of calculation of the unidirectional function (e.g. Traw, col. 7, lines 5-55).

In respect to claims 15-16, the claim limitations are similar to claims 9-11. Therefore claims 15-16 are rejected based on the similar rationale.

In respect to claim 17, Traw and Jones disclose the information processing system as claimed in claim 6, wherein the first information processing apparatus and the second information processing apparatus generate either one of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, and generate the encryption key of the other transmission mode on the basis of the generated encryption key; the generated random number and the received random number (e.g. Traw, col. 3, lines 10-30).

In respect to claims 18-27, the claim limitation is similar to claim 7-16. Therefore claim 18 is rejected based on the similar rationale.

In respect to claims 31-54 and 58-81, the claim limitations are similar to system claims 1-27. Therefore, claims 31-54 and 58-81 are rejected based on the similar rationale.

In respect to claims 28, 55 and 82, the claim limitations are similar to claim 1. Therefore, claims 28, 55 and 82 are rejected based on the similar rationale.

### ***Conclusion***

Art Unit: 2134


4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-3962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

  
Examiner: Tongoc Tran  
Art Unit: 2134

March 30, 2006

  
JOSEPH H. LOUIS  
PATENT EXAMINER